Soldiers Online

Beware the Id

Story by Sandy Goss

THESE are the details of the case as events unfolded:

In October 1999, the Army Criminal Investigation Command, or CID, received complaints that unauthorized credit card accounts had been opened in the names of several general officers. Special agents contacted the Secret Service, an element of the Treasury Department having jurisdiction over credit-card fraud, and alerted it to the problem.

The Secret Service then set up a joint task force that included investigators from the CID, the Naval Criminal Investigative Service and the Air Force Office of Special Investigations.

The four agencies set out to find those responsible for applying for and obtaining hundreds of credit cards in the names of top U.S. military officers, including more than 175 generals and admirals.

The investigation revealed that the perpetrators of the fraud had accessed the Internet for the information. Once the information was obtained, they used the data to apply for unauthorized credit under the victims' names and make purchases over the Internet.

The initial CID portion of the investigation revealed some 200 Army officers who were the victims of identity theft. The task force identified almost 1,300 fraudulent accounts opened in officers' names. Potential losses could have reached an estimated $1.4 million if the accounts had been drained to their limit, officials said.

Investigators learned that most of the fraudulent credit cards were issued by one particular bank. The bank said its routine monitoring detected the fraudulent accounts and that most of the accounts were closed within 24

Sandy Goss works for the CID Public Affairs Office at Fort Belvoir, Va.

entity Thieves

hours of being created. The bank also said its losses from this fraud were small and that it was certain it had identified all the fraudulently obtained accounts.

On Dec. 13, 1999, Secret Service agents from field offices in Newark, N.J., and Philadelphia, Pa., in conjunction with the Trenton, N.J., Police Department, arrested three non-Department of Defense civilians in Trenton and a fourth suspect in Philadelphia. All four were charged with conspiracy to commit bank fraud — a violation of Title 18 of the U.S. Criminal Code, Section 371.

The four are accused of using 113 unauthorized credit card accounts to make $37,000 in Internet purchases. Each individual faces a maximum penalty of 30 years imprisonment and fine of up to $1 million. U.S. attorneys in Delaware, New Jersey and Pennsylvania will prosecute the case. Additional suspects have been identified.

A Growing Problem

This investigation represented one of the most comprehensive Army criminal cases of its type, proving once again that identity theft can be one of the decade's most profitable crimes.

The U.S. Public Interest Research Group has said that identity theft claims about 40,000 new victims each year. The "Identity Theft Act" of 1998 makes it a federal offense.

The Personal Hassle of ID Theft

Although victims of identity theft are not normally financially liable, they may incur legal bills and suffer personal embarrassment, in addition to the time lost and inconvenience associated with repairing their credit records.

They nevertheless must go through the tedious process of reviewing their credit ratings and checking their old financial statements. Sometimes the damage caused due to fraud goes undiscovered for months and the victim is alerted only after applying for credit or receiving letters from collection agencies.

Even when victims' credit is initially believed to be repaired, they can experience additional credit problems caused by derogatory entries left in various obscure financial or credit files.

To lessen subsequent vulnerability to such fraud, victims and potential victims are eliminating their Social Security numbers from potentially compromisable documents such as their checks.

One twist to this crime is that — unlike the theft of an existing credit card, where the victim knows that the card is missing — these victims had no idea that they'd been compromised. They were unaware that cards had been issued in their names because the charges made on the fraudulently obtained cards didn't appear on their legitimate monthly statements. The bogus cards and their monthly statements were sent to postal boxes and other neutral addresses in various states.

Why Target the Military?

Career officers and NCOs tend to have very good credit histories, and this is even more true as individuals advance in rank. In a downsizing and highly competitive military environment, clean credit records are important in terms of promotion potential. However, they also garner the higher credit limits that appeal to thieves.

Blame It On the Internet

The increase in identity-theft crimes has paralleled advances in information technology. It has always been axiomatic that tearing up credit card carbons and safeguarding sales receipts were necessary precautions to prevent credit-card fraud.

Today, however, the practice of selling, posting and transmitting personal information via the Internet has made personal data increasingly vulnerable and accessible.

Competent crooks can get personal information from websites, retrieve it from public databases, or obtain it through Internet and phone solicitation. Criminals may also get personal information by stealing mail, wallets or purses; by rummaging through personal trash; and through credit application fraud or unethical employee

Checking Your Credit Report

THREE major credit-reporting agencies provide credit report information for a nominal fee, and they should be contacted to report any fraudulent use of your credit accounts. The agencies are:

Equifax, (800) 525-6285, **www.equifax.com**
Experian, (888) 397-3742, **www.experian.com**
Trans Union, (800) 680-7289, **www.tuc.com**

The increase in identity-theft crimes has paralleled advances in information technology.

transactions. Once acquired, personal information can allow access to a wide range of financial accounts.

Protect Personal Information

You can avoid or deter identification theft by carefully protecting your personal information. There are several ways to avoid becoming a victim of identity fraud.

• Guard your Social Security number and other identification numbers. Only give them to people you trust.

• Don't give out personal information over the telephone, through the mail or over the Internet unless you have initiated the contact or know the person with whom you're dealing.

• Each year, purchase copies of your credit reports and check them for errors. See the accompanying box for phone numbers and websites of the three major credit-reporting agencies. Charges for the service run to about $8.50 per report.

• When paying by credit card in a store, keep the card in sight; make sure that you can see it being swiped through the machine.

• To have your name removed from mailing lists for credit card offers, call the toll-free number used by the three major credit bureaus: (888)-5OPTOUT [(888) 567-8688].

• Use a shredder to destroy charge receipts, copies of credit applications, insurance forms, bank checks and statements that you are discarding. Also destroy expired charge cards and card offers received in the mail.

• Make it a habit to shred other personal documents that may contain key information about you.

• At work, find out who has access to your personal information and verify that the records are secure.

• Do not post personal information on bulletin boards or Internet sites.

• Ensure that commerce sites are legitimate and have transaction security before purchasing online.

• Check monthly credit and bank statements item by item and order a credit report at least once each year.

• Exercise your right to stop "credit header" information (personal information label on a credit report) from being sold to merchants. This will also stop pre-approved credit card offers. To exercise this option, call the Automated OptOut Request Line number listed above.

Victims, Take Action

If you discover that you're a victim of identity theft, there is action you can take:

• Report the crime to military or civilian police, as appropriate, and ask for a copy of the police report to document the crime.

• Alert the security departments of appropriate creditors or financial institutions through which the

Identity Theft: The FAQs

Q: You cite three credit reporting agencies: Equifax, Trans Union and Experian. Are there service centers outside the continental United States to contact? Toll-free 800 numbers are expensive phone calls from over here.

A: At press time, CID did not have OCONUS numbers for these three service centers. Perhaps the best way to contact the credit-reporting agencies from overseas is through the Internet.

Q: Can you give us OCONUS-based contact information for the Federal Trade Commission or other agencies for consumer complaints?

A: You can file a complaint with the FTC by contacting the Consumer Response Center by phone [toll-free at (877) FTC-HELP (382-4357)]; by mail to Consumer Response Center, Federal Trade Commission, 600 Pennsylvania Ave., NW, Washington, DC 20580; or through the

accounts were fraudulently accessed or opened.

• Close these accounts and place passwords on any new and existing accounts. (Don't use easily available information such as your mother's maiden name, your birth date, the last digits of your Social Security or phone number, or a series of consecutive numbers when choosing new passwords.)

• Also alert the fraud departments of each of the three major credit-reporting agencies

• Ask to have a "fraud alert" placed on your file, so that new credit will not be granted without your approval.

• Keep meticulous records of all attempts to clean your records. This should include copies of letters and summaries of your phone conversations with credit officials.

• Never agree to pay any portion of the fraudulent debt, since this will cause the balance to remain on your record.

• Seek legal assistance to ensure you have taken advantage of the resources available to help you resolve credit problems.

• Call the Federal Trade Commission's toll-free Identity Theft Hotline at (877) IDTHEFT [(877) 438-4338] or visit its website, **www.consumer.gov/idtheft**.

The publication "ID Theft: When Bad Things Happen to Your Good Name" is available through either the Identity Theft Hotline or from its website.

Insurance Protection Available

A new type of insurance, offered in 25 states, covers some of the expenses incurred by identity fraud victims. This coverage can be added to existing homeowners' or renters' policies and provides reimbursement of up to $15,000 for each instance of fraud. Covered expenses include lost wages for taking time off from work to deal with the fraud, legal fees, certain mailing costs, loan reapplication fees and phone charges.

The coverage includes identity fraud resulting from Internet use.

While the Fair Credit Billing Act generally limits a consumer's liability for unauthorized credit card charges to $50 per card, the ultimate costs may be substantial. Check with your insurance company for availability of this coverage. □

Internet, using the online complaint form at **www.ftc.gov**. The FTC cannot resolve individual problems for consumers, but it can act against a company if it determines a pattern of possible law violations exists.

Q: Who should I contact when reporting cases of fraud?

A: That depends on the specific case. Determining factors such as where the crime was committed, who may have committed the crime and the dollar amount of the loss all affect which police jurisdiction has primary responsibility. Generally, if the crime involved an Army suspect or occurred on Army-controlled property or equipment, the MPs or CID take the complaint. However, the incident might be referred to another agency having greater jurisdictional responsibility, such as the local national police (if overseas), U.S. Secret Service or postal inspectors.

Q: People shopping over the Internet are told to "use caution when disclosing checking account numbers, credit card numbers or other personal financial data on any website or online service location." Can you be more specific?

A: There are several good sites that offer tips on how to make your communications more secure when shopping online. Almost all of the Internet service providers give their customers tips on how to be secure when shopping online, and most offer a secure means of communication. Here are additional tips:

• Use only one credit card online, to make it easier to identify fraudulent charges.

• Use only a credit or charge card — never a bank debit card — for online purchases. Under the Fair Credit Billing Act, credit cards have liability limits on them, and under certain circumstances consumers can dispute charges or withhold payment while their accounts are being investigated. Debit cards don't offer such protection, and using one online puts your entire checking or savings account at risk.

• Print a copy of your purchase order and confirmation number for your records whenever you make a purchase online.

• Check your bills carefully each month and cancel the card immediately if you find any false or fraudulent charges.

• Use caution when disclosing checking account numbers, credit card numbers or other personal financial data at any website or online service location, unless you receive a secured authentication key from your provider.

• When you enter an interactive service site, beware of con artists who may ask you to "confirm" your enrollment service by disclosing passwords or the credit card number you used to subscribe.

Q: Are there force-protection issues of ID theft that I should know about?

A: Anything that affects a person's readiness could be considered force protection related. This includes financial problems or time away from work caused by identity theft.

Q: What else can I do to protect myself from identity theft?

A: Don't leave personal records or documents that contain Social Security numbers — a whole range of cards and papers you might carry in your wallet or purse — lying around for others to see, and be very careful about who you give personal information, and how you do so. Just as you wouldn't leave your unattended automobile unlocked with the keys in it, you should never leave your identity unsecured. — *CW5 Guy Surian, chief of current operations, HQs., CID*